Screencast: 19-logging.webm or 19-logging.mp4

REFERENCES

LaUSAH - Chapter 10, Logging
RHEL7 System Aministrators Guide, Chapter 23, Viewing and Managing Log Files (PDF in weekly content)

RSYSLOG

Rather than each service / daemon having their own logging features, a general purpose logging service was created.
RHEL/CentOS provides a package named rsyslog that includes the rsyslogd daemon.
Most all logs are stored under /var/log/ or within a sub-directory.

SAMPLE `/etc/rsyslog.conf`

```
*.info;mail.none;authpriv.none;cron.none /var/log/messages
authpriv.* /var/log/secure
mail.* -/var/log/maillog
cron.* /var/log/cron
*.emerg *
uucp,news.crit /var/log/spooler
local7.* /var/log/boot.log
```

LOGROTATE

Logrotate allows for the automatic rotation, compression, removal and mailing of log files.
Logrotate can be set to handle a log file daily, weekly, monthly or when the log file gets to a certain size.
Normally, logrotate runs as a daily cron job.

LOGROTATE FILES

Runs as a cron job:
  `/etc/cron.daily/logrotate`
Config files:
  `/etc/logrotate.conf` (compress)
  `/etc/logrotate.d/*` (service specific logrotate configs)
Note: Most services include a specific logrotate config.

```
[root@sdowdle ~]# rpm -qc httpd | grep logrotate
 /etc/logrotate.d/httpd
```

EXAMPLE ROTATED LOGS

```
[root@esus ~]# ls -lh /var/log/messages* (from older system)
-rw------- 1 root root 80K Sep 29 08:53 /var/log/messages
-rw------- 1 root root 12K Sep 26 04:03 /var/log/messages.1.gz
-rw------- 1 root root 11K Sep 19 04:02 /var/log/messages.2.gz
```

```
[root@sdowdle ~]# ls -l /var/log/messages*
-rw------- 1 root root 464 Sep 29 10:18 /var/log/messages
-rw------- 1 root root 10089 Sep 26 03:29 /var/log/messages-20200926
```

LOGWATCH

Logwatch is a customizable, pluggable log monitoring system.
Runs as a cron job: /etc/cron.daily/0logwatch
It will go through your logs for a given period and make a report in the areas that you wish with the detail that you wish.
By default the logrotate package will email the root user a report every morning.

USEFUL COMMANDS

`tail` - output the last part of files
  `-f` flag is for follow... watch a log file as it grows
`grep` - search a log file
`zgrep`, `zless` and `zcat` - for compressed log files

sysstat - provides `sar` and `iostat`

> `sar` and `iostat` enable system monitoring of disk, network, and other IO activity by parsing the binary log data collected every 10 minutes.
> By default, systat runs as a cron job.

journald

RHEL7 introduced the systemd init system. systemd includes a new logging facility named journald.
journald can be run in parallel with rsyslog or as a replacement for it.
The command used to access the journald binary log files is journalctl.
For a regular user to access logging data via journalctl, add them to the adm group.

SESSION VS PERSISTANT

journald by default stores log data in RAM.
To enable persistant storage just create a directory named journal in /var/log if it doesn't already exist and then restart the systemd-journald service or reboot.

JOURNALD FEATURES

- Gets all of boot and shutdown.
- More log data
- kernel, user processes, and from STDIO and STDOUT
- Includes extensive metadata info
- All logged data are shown including rotated logs.
- journalctl offers database-like queries.
- journalct offers some tab completition features.
- Graphing of boot up showing service start up times.

journalctl Examples

```
journalctl -n Number
journalctl -p Priority
journalctl -u Unit
journalctl -f (like tail -f)
journalctl --since=value --until=value
journalctl --disk-usage
```

journalctl presentation video by Lennart Poettering

https://www.youtube.com/watch?v=i4CACB7paLc